

REMARKS

The applicant has carefully considered the Examiner's non-final rejection based on the cited prior art. The applicant submits that the claims, as amended, patentably distinguish the invention over the cited prior art for the following reasons:

Claim objections

The Examiner noted that line 6 of claim 1 required correction of an antecedent reference. This claim has been amended in accordance with the Examiner's suggestion.

The pending claims are patentable over the AAPA and Davis (U.S. Patent No. 5,937,063)

In the Detailed Action dated September 7, 2007 (the "Detailed Action"), all pending claims were rejected under 35 U.S.C. 103(a) as being unpatentable over the alleged Applicant's Admitted Prior Art (AAPA) in view of Davis. The Applicant traverses this rejection and submits that the pending claims are patentable over the AAPA and Davis for the reasons below.

The AAPA does not disclose "either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein"

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970).

In the Detailed Action, paragraph 7, page 3, it is asserted that the AAPA:

teaches a boot method for use in a mobile device having a FLASH memory storing content comprising boot instructions (External Memory (FLASH) 18, figure 1 of the instant application), an internal-read only memory storing boot program code (BootTOM 14, figure 1 of the instant application), and having a serial port (serial port 12), execution of the boot program code stored in the read-only memory causing the mobile device to perform the steps of:

either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein (figure 2 of the instant application and paragraphs [0003]-

[0006]).

However, no such admission is made by the Applicant; the alleged AAPA makes no such disclosure. Figure 2 of the instant application is not a prior art description; it is introduced at paragraph [0024] of the Detailed Description. Paragraphs [0003] to [0005] of the instant application describe that:

[0003] ... Typically, a mobile device comprises a reset switch, or other equivalent means known in the art, which a user can actuate in order to initiate a reset response.

[0004] ... An external reset switch typically controls a reset circuit in the mobile device. When the reset switch is actuated, the reset switch is actuated, the reset circuit closes, sending a signal, or reset command, to the ASIC to reset. **When the reset switch is released** and the reset circuit opens, instructions stored in internal BootROM are executed **and the BootROM instructs the ASIC to poll a serial port**, which can be connected to a personal computer, for activity.

[0005] If there is serial port activity, this usually indicates that there is new code to be downloaded. This new code may be stored in memory on a personal computer.... Typically, program code in the BootROM will jump to a routine for downloading the new code via the serial port into internal SRAM... **This constitutes a potential security risk, since it can allow anyone to provide new code at the serial port that, once executed, can access and upload programs and data stored in the mobile device's FLASH memory**, including confidential and proprietary information. Such access would constitute a security breach. (emphasis added)

Nowhere in paragraphs [0003] to [0006] is it admitted that “either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein” is prior art. Rather, it is pointed out in paragraph [0004] that when a “reset switch is released... the BootROM instructs the ASIC to poll a serial port”; there is no option to poll the serial port in place of “jumping to the FLASH memory”; the serial port is always polled, as explained in paragraph [0004]. The inevitable polling is the reason why the potential security risk is described in paragraph [0005].

Further, it is acknowledged in the Detailed Action, paragraph 7, page 3, that the following does **not** constitute AAPA:

... the FLASH memory storing a key value stored in security location, and internal read-only memory storing a predetermined value:

reading the key value from a security location in the FLASH memory, the key value being independent of the content of the FLASH memory;

comparing the key value to a predetermined security value stored in the internal read-only memory, the predetermined security value being independent of the content of the FLASH memory; and

depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein.

Thus, it is acknowledged that “either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein” is **not** prior art.

In the Detailed Action, paragraph 7, page 4, it is asserted that Davis discloses, *inter alia*, “comparing the key values to a predetermined security value stored in the internal read-only memory” and “depending on the result of the comparison of the key value to the predetermined value jumping to the FLASH memory for execution of boot instructions stored therein”.

However, Davis does not disclose these elements.

The cited passages of Davis do not disclose a “comparing” process. In column 2, lines 33-55 of Davis, it is stated that:

... the secure boot device responds to the requests from a host processor... by encrypting the instruction code in the boot-up program using a secret key shared with the host processor. The encrypted instruction code is decrypted by the host processor using the same secret key. The encrypted instruction code is decrypted by the host processor using the same secret key. Since the secret key is known only by the host processor and the secure boot device, any attempt to replace the secure boot device containing the boot-up program, will result in incorrect decrypted code making the system inoperable.

There is thus no “comparing” of the secret key of Davis to another value; the key is used to encrypt instruction code, which is subsequently decrypted.

Furthermore, there is no disclosure of “depending on the result of the comparison of the key value to the predetermined value jumping to the FLASH memory for execution of boot instructions stored therein”, inasmuch as there is no “comparison of the key value to the

predetermined value”, as set out above. However, to be precise, this is not the language of any of the independent claims; what claim 1 recites, specifically, is:

depending on the result of the comparison of the key value to the predetermined security value, **either polling the serial port for activity or** jumping to the FLASH memory for execution of boot instructions stored therein.

Thus, claim 1 provides for the specific alternative that **either** “polling the serial port for activity” is carried out, **or** that “jumping to the FLASH memory...” is carried out. Davis, however, does not disclose such an alternative; Figure 2 of Davis, for example, only provides that if there is a “valid boot-up instruction” (12), the “host processor processes boot-up instruction until done” (14). Figure 2 of Davis does not provide “polling the serial port for activity” in the alternative.

Thus, it is submitted that claim 1 is patentable over the cited prior art, as neither the AAPA nor Davis, separately or in combination, discloses each of the elements of claim 1. A *prima facie* obviousness rejection has not been established, inasmuch as the cited prior art fails to disclose all of the elements of the claim.

Similarly, the Applicant submits that claim 8, which recites a processor configured to execute boot program code “for comparing said key value to a predetermined security value stored in the internal read-only memory wherein said predetermined security value and said key value are each independent of other content stored in the FLASH memory, and, depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the flash memory for execution of boot instructions stored therein”; claim 9, which recites an apparatus comprising a processor being configured to “compare the key value to the predetermined security value, and, depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein”; claim 18, which recites “executing instructions stored in the BootROM code to compare the key value to a predetermined security value stored in the BootROM memory, the predetermined security value being independent of the other content stored in the FLASH memory” and “on the condition that the comparison shows a match between the key value and the predetermined security value, executing instructions stored in the BootROM code to transfer execution to instructions stored in a boot location in the FLASH memory; and on the condition that the comparison shows a

mismatch between the key value and the predetermined security value, polling the serial port for activity”; claim 19, which incorporates claim 18 by reference; and claim 20, which recites BootROM code comprising instructions executable on a processor to “compare the key value to a predetermined security value stored in the BootROM memory, the predetermined security value being independent of the other content stored in the FLASH memory; on the condition that the comparison indicates a match between the key value and the predetermined security value, transfer processor execution to instructions stored in a boot location in the FLASH memory; and on the condition that the comparison shows a mismatch between the key value and the predetermined security value, poll the serial port for activity” are all patentable over the cited prior art for the same reasons given above with respect to claim 1.

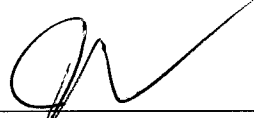
Since the cited art fails to render any of the independent claims obvious, all the dependent claims are nonobvious as well. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988).

Further, with specific reference to claim 2, the Applicant submits that contrary to the assertion in the Detailed Action, paragraph 8, it would not have been obvious to a person of ordinary skill in the art to modify the AAPA to perform polling “if the key value does not match the predetermined security value”, inasmuch as the cited prior art fails to disclose the use of a key value that is compared to a predetermined security value, as discussed above.

No new subject matter has been added by this amendment. Favourable reconsideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on December 6, 2007.

RICHARD C. MADTER
RYAN J. HICKEY
CHRISTOPHER PATTENDEN



Jenna L. Wilson
Registration No. 54908
(416) 971-7202, Ext. 290

Customer Number: 38735